IN THE CLAIMS

Please amend the claims as follows:

1. (Previously Presented) A public key authentication system for use in a computer system having a plurality of users, the system comprising:

a virtual smart card server;

storage connected to the virtual smart card server, wherein the storage includes a plurality of virtual smart cards, wherein each virtual smart card is associated with a user and wherein each smart card includes a private key; and

a virtual smart card agent connected to the virtual smart card server, wherein the virtual smart card agent includes a user authentication interface for use by a user in entering a one-time password, wherein the virtual smart card agent authenticates the user using the one-time password and accesses the authenticated user's virtual smart card to obtain the user's private key.

2. (Original) The public key authentication system according to claim 1, wherein the virtual smart card agent includes an interface to a smart-card-enabled application.

3. (Original) The public key authentication system according to claim 2, wherein the virtual smart card server performs encryption in response to a remote call from the interface.

4. (Original) The public key authentication system according to claim 2, wherein the virtual smart card server performs signing in response to a remote call from the interface.

5. (Original) The public key authentication system according to claim 2, wherein the virtual smart card server performs key management functions in response to a remote call from the interface.

COPY

6. (Original) The public key authentication system according to claim 1, wherein the public key authentication system further includes an authentication server connected to the virtual smart card agent and wherein the virtual smart card agent authenticates the user through interaction with the authentication server.

7. (Previously Presented) The public key authentication system according to claim 1, wherein the public key authentication system further includes an authentication server connected to the virtual smart card server, wherein the authentication server includes means for authenticating a user using a one-time password authentication token.

8. (Original) The public key authentication system according to claim 1, wherein the virtual smart card agent communicates with the virtual smart card server over an agent-server transport layer.

9. (Original) The public key authentication system according to claim 1, wherein the virtual smart card agent communicates with the virtual smart card server over a secure TCP/IP session.

10. (Original) A method of authenticating users, including a first user, attempting to access a computer system, the method comprising:

assigning first and second keys to each user, wherein the first and second key form a public/private key pair;

issuing a digital certificate to the first user, wherein the digital certificate is associated with the second key assigned to the first user;

entering a one-time password;

encrypting the one-time password with the first key assigned to the first user to form an encrypted one-time password;

verifying that the digital certificate issued to the first user was signed by a recognized certificate authority;

accessing, via the digital certificate, the second key assigned to the first user;

COPY

decrypting the encrypted one-time password with the second key associated with the digital certificate to recover the one-time password; and

comparing the one-time password against an expected one-time password.

11. (Original) The method according to claim 10, wherein the first key is a private key and the second key is a public key.

12. (Original) The method according to claim 10, wherein verifying that the digital certificate issued to the first user was signed by a recognized certificate authority includes accessing a CRL to determine if the certificate has been revoked.

13. (Original) A computer-readable medium comprising program code which executes the method of claim 10.

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Previously Presented) The method of claim 1, wherein entering a one-time password includes displaying the one-time password on an authentication token.